Texas Department of Information Resources
CYBER SECURITY TIPS
Monthly Newsletter
Office of the Chief Information Security Officer July 2008 | Volume 2, Issue 7

What is a Data Breach?

A data breach generally refers to instances where information has been subject to unauthorized access, often where the information is lost, stolen, or hacked into. This is of particular concern when that information is private, sensitive, or confidential. Organizations and individuals are responsible for protecting the information in their care, so proper safekeeping of this data is vital. Failure to do so can result not only in a breach but also in damage to reputation, significant fines or loss of revenue, and other negative consequences.

Data breaches occur all too frequently, and they can occur in large or small organizations in both the public and private sectors. The scope of this issue can be evidenced by the fact that more than 227 million records nationwide have been involved in breaches since February 2005. This figure represents only those that have been reported, so it may reflect only a portion of the actual occurrences. This is an issue that everyone must be aware of and take steps to mitigate.

We must also recognize that data manipulation is a potential threat. If we cannot trust the integrity of our data and know that it has not been altered inappropriately, our ability to carry out our mission and serve our customers becomes impaired.

Some examples of data that must be protected include:

- Customer or employee information with names, addresses, Social Security numbers, credit card numbers, passwords, and other identity-related information
- Intellectual property
- Financial information
- Health records of individuals

HOW IS DATA COMPROMISED OR DISCLOSED?

Attempts by hackers to steal names, Social Security numbers, credit card accounts, and other information are one method of obtaining data. Attackers may use social engineering, phishing, or other similar attempts to gain access. These activities can translate into very large sums of revenue for those in the organized crime world. While very sophisticated techniques are sometimes used to steal sensitive data, one of the most common threats comes from within the organization itself. According to Deloitte's 2007 Global Security Survey, 65% of respondents reported repeated external breaches. Of those incidents, 18% stemmed from unintentional data leakage. The report also indicates that some of the surveyed data breaches went undetected for extended periods. According to the 2008 Data Breach Investigations Report by VerizonBusiness, 83% of attacks were not highly difficult and 87% of breaches were considered avoidable through *reasonable controls*. A full report is available for download at **www.verizonbusiness.com/resources/security/databreachreport.pdf**.

The loss or theft of data is not limited to electronic data loss or computer hacking. Other possibilities include physical loss of hard copy documents, theft or loss of laptops, tapes and flash-drive devices, or improper disposal of hardcopy documents.

DO LAWS OR REGULATIONS TO PROTECT DATA EXIST?

Numerous laws and regulations control how organizations handle and protect sensitive information including:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Payment Card Industry (PCI) Security Standard
- Gramm-Leach-Bliley Act (GLBA – applies only to financial institutions)
- Sarbanes-Oxley Act (SOX – applies only to public companies)

Breach Notification Laws are currently in place in forty-two states and the District of Columbia. They govern the notification of an individual whose personal information has or may have been disclosed.

Texas Business & Commerce Code, Chapter 48, provides for notification requirements following breach of security of computerized data. See **tlo2.tlc.state.tx.us/statutes/docs/BC/content/pdf/bc.004.00.000048.00.pdf** as well as the State Security Breach Notification Laws: **www.ncsl.org/programs/lis/cip/priv/breachlaws.htm**.

WHAT CAN I DO?

Organizations and individuals must take proactive measures to minimize the risk of data breach. Everyone in an organization has a role in protecting information. The following examples offer advice on how to help prevent data disclosure:

- Follow your organization's cyber/information security policies.
- Know how your organization has classified information, and adhere to the appropriate controls in place.
- Follow proper procedures for the destruction or disposal of media that contains sensitive data.
- Participate in security awareness training.

Remember, cyber security is everyone's responsibility. Don't be the weak link in the chain.

ADDITIONAL RESOURCES

The following sites offer additional guidance regarding data breaches:

- Data Spill **en.wikipedia.org/wiki/Data_spill**
- A Chronology of Data Breaches **www.privacyrights.org/ar/ChronDataBreaches.htm**
- Dealing with a Data Breach: **www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html**
- Data Loss Cost Calculator: **www.tech-404.com/calculator.html**

For previous issues of the Monthly Cyber Security Tips Newsletter, please visit **www.dir.state.tx.us/security/reading**.

For more information on Internet security, please visit the SecureTexas website – **www.dir.state.tx.us/securetexas**. SecureTexas provides up-to-date technology security information as well as tips to help you strengthen your part of Texas' technology infrastructure. Report serious information security incidents as quickly as possible to your agency's Information Security Officer and to DIR's 24/7 Computer Security Incident Notification hotline: (512) 350-3282.

Brought to you by: MS-ISAC
www.msisac.org

Powered by: US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM
www.us-cert.gov

Distributed by: DIR Secure Texas
www.dir.state.tx.us/securetexas